UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/457,914 | 12/10/1999 | GERMANO CARONNI | 06502.0289 | 8208 |

22852 7590 09/23/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/457,914 | CARONNI ET AL. | |
| | Examiner | Art Unit | |
| | LEYNNA T. HA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,5-20,22-37 and 39-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-20, 22-37, and 39-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 13, 14, 10
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

**1.** Claims 1-3, 5-20, 22-37, and 39-45 have been re-examined and Applicant have canceled claims 4, 21, and 38.

**2.** Claims 1-3, 5-17, 18-20, 22-37, and 39-45 have been rejected under 35 U.S.C. 103(a), necessitated by new grounds of rejection.

**3.** This is a Non-Final rejection.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

***4. Claims 1-3, 5-17, 18-20, 22-37, and 39-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devine, et al. (US 6,606,708).***

**As per claim 1:**

Devine, et al. teaches a method executed in a data processing system for providing communication access between a first process and a second process comprising:

appending security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

transmitting a packet from the first process to the second process through the open socket, the packet comprising the security context information for the first process in the process table; and **(col.14, lines 6-11)**

determining if the first and second process belong to a channel; and **(col.9, lines 1-21 and col.20, lines 53-63)**

accepting the transmitted packet when the first and second process belong to the channel. **(col.22, lines 53-67 and col.23, lines 7-16)**

**[Devine discloses once the client session is determined to be secure and the message with valid security information, the user is entitled to communicate with the desired connection. It is obvious the session is mapped to the targeted destination for Devine discloses that the validation is performed to make sure that the user is entitled to communicate with the desire service (col.9, lines 1-21). Further, since the request is mapped to the associated session, it is obvious that the**

**session refers to a target system, which is the associated to a channel, destination/target address, and socket that belongs to the associated target system. Plus, Devine discloses a key is necessary to validate the first and second process, which the key identifies and validates the particular process that obviously allows communication to the associated system. Thus, it would have been obvious to determine if the process belongs to a channel and accepting the transmitted packet that belong to the channel is establishing that the session is secure by having the proper key that identifies the associated session.]**

**As per claim 2:**

Devine discusses modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

**As per claim 3:**

Devine discloses receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

**As per claim 5:**

Devine discloses the method of determining if the first and second process belong to a channel includes:

comparing the security context information in the received packet and security context information in another process table. **(col.27, line 43 thru col.28, line 5)**

**As per claim 6:**

Devine discloses the process table and another process table are located on a single node. **(col.9, lines 60-66)**

**As per claim 7:**

Devine discloses the method of verifying the security context information includes:

determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

**As per claim 8:**

Devine discloses the method of determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

**As per claim 9:**

Devine discloses the method of permitting use of the packet includes decrypting the packet on a node and **(col.8, lines 27-28)** authenticating a sender associated with the first process on the node **(col.12, lines 34--37)**.

**As per claim 10:**

Devine discloses the method of appending security context information comprises:

obtaining the security context information from a third process, the security context information comprising a virtual address and a node identification; and **(col.9, lines 2-10 and col.14, lines 6-11)**

limiting each of the first, second and third processes to communicate with another process provided that the communication processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

**As per claim 11:**

Devine discloses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

**As per claim 12:**

Devine teaches a method for placing processes executed in a node in security context, comprising :

sending a request from the node to a server to verify username and node identification associated with a process; **(col.14, lines 7-11)**

in response to the request, receiving security context information at the node from the server, the security context information comprising a virtual address for the node; **(col.22, lines 25-30 and lines 53-66 and col.23, lines 61-64)**

initiating the process, and **(col.10, lines 38-41)**

appending the security context information and the node identification associated with the process in a process table. **(col.13, line 43 thru col.14, line 17)**

**[The message includes the user identifier (username) and the virtual address. In addition, the session information, proxy specific data, and the target proxy identifier (col.13, lines 48-67) and the socket type and port number of which identifies the node (col.26, lines 24-29). It is obvious that a secure session comprises the message include a node identification and an address in order to identify and determine the proper system that it is communicating to, else the session would be not be considered secure (col.11, lines 41-43).]**

**As per claim 13:**

Devine discusses receiving security context information further includes receiving a key that corresponds to the node identification from the server. **(col.8, lines 52-55)**

**As per claim 14:**

Devine discusses the method of claim 13, further comprising:

encrypting a packet transmitted by the process using the key;

**(col.9, lines 6-13)**

encapsulating the encrypted packet with a header that comprises the node identification. **(col.13, lines 31-67) (col.9, lines 6-13)**

**As per claim 15:**

The method of claim 12, further comprising:

sending a second request from the node to the server to verify username and node identification; **(col.10, lines 39-44)**

receiving additional security context information comprises from the server, wherein the additional security context information includes a second virtual address for the node; **(col.23, lines 61-63)**

creating a second process; and **(col.24, lines 60-64)**

appending the security context information for the second process in the process table that is associated with the second process. **(col.13, line 43 thru col.14, line 17)**

**As per claim 16:**

Devine teaches a method executed in a data processing system for providing secure communications between a first process and a second process, comprising:

obtaining node identification and a virtual address; **(col.9, lines 2-10 and col.23, lines 61-64)**

**[The message includes the user identifier (username) and the virtual address. In addition, the session information, proxy specific data, the target proxy identifier (col.13, lines 48-67), and the socket type and port number of which identifies the node (col.26, lines 24-29). The message includes a node identification and an address in order to identify and**

**determine the proper system that it is communicating to, else the session would be not be considered secure (col.11, lines 41-43).]**

including the node identification and the virtual address in a field corresponding to the first process in a process table; **(col.14, lines 7-11 and col.23, lines 61-63)**

transmitting a datagram that contains the node identification and the virtual address from the first process to a socket; and **(col.24, lines 60-64)**

receiving the datagram at the second process that contains the node identification and a second virtual address. **(col.14, lines 7-11 and col.23, lines 61-64)**

**As per claim 17:**

Devine teaches the method of claim 16, wherein obtaining a node identification and a virtual address further comprises:

modifying a socket structure in the socket so that the socket structure accepts the node identification and the virtual address; and **(col.13, lines 31-67)**

modifying a process table so that the table comprises a node identification field and a virtual address field. **(col.23, lines 26-31 and col.26, lines 24-31)**

**As per claim 18:**

Devine teaches a system for providing communication access between a first process and second process, comprising:

means for appending security context information for the first process in a process table; **(col.9, lines 60-63 and col.13, lines 60-67)**

means for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

means for transmitting a packet from the first process to the second process through the open socket, the packet comprising the security context information for the first process in the process table; **(col.14, lines 6-11)**

means for determining if the first and second process belong to a channel; and **(col.9, lines 1-420, lines 53-63)**

means for accepting the transmitted packet when the first and second process belong to the channel. **(col.22, lines 53-67 and col.23, lines 7-16)**

**[Devine discloses once the client session is determined to be secure and the message with valid security information, the user is entitled to communicate with the desired connection. It is obvious the session is mapped to the targeted destination for Devine discloses that the validation is performed to make sure that the user is entitled to communicate with the desire service (col.9, lines 1-21). Further, since the request is mapped to the associated session, it is obvious that the session refers to a target system, which is the associated to a channel, destination/target address, and socket that belongs to the associated target system. Plus, Devine discloses a key is necessary to validate the first and second process, which the key identifies and validates the**

**particular process that obviously allows communication to the associated system. Thus, it would have been obvious to determine if the process belongs to a channel and accepting the transmitted packet that belong to the channel is establishing that the session is secure by having the proper key that identifies the associated session.]**

**As per claim 19:**

Devine discloses means for modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

**As per claim 20:**

Devine discloses means for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

means for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

means for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

**As per claim 22:**

Devine discloses the system of claim 21, wherein means for determining if the first and second process belong to a channel comprises:

means for comparing the security context information in the received packet and security context information in another process table. **(col.27, line 43 thru col.28, line 5)**

**As per claim 23:**

Devine discloses the system of claim 22, wherein the process table and the another process table are located on a single node. **(col.9, lines 60-66)**

**As per claim 24:**

Devine discloses the system of claim 20, wherein means for verifying the security context information comprises:

means for determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

means for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

**As per claim 25:**

Devine discloses a system of claim 24, wherein means for determining whether the first and second process belong to two different linked channels comprises:

means for initiating a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

**As per claim 26:**

Devine discloses the system of claim 24, wherein means for permitting use of the packet comprises:

means for decrypting the packet on a node; and **(col.12, lines 34--37)**.

means for authenticating a sender associated with the first process on the node. **(col.8, lines 27-28)**

**As per claim 27:**

Devine includes the system of claim 18, wherein means for appending security context information includes:

means for obtaining the security context information from a third process including a virtual address and a node identification; and

**(col.9, lines 2-10 and col.23, lines 61-64)**

**[The message includes the user identifier (username) and the virtual address. In addition, the session information, proxy specific data, and the target proxy identifier (col.13, lines 48-67) and the socket type and port number of which identifies the node (col.26, lines 24-29). It is obvious that a secure session comprises the message include a node identification and an address in order to identify and determine the proper system that it is communicating to, else the session would be not be considered secure (col.11, lines 41-43).]**

means for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

**As per claim 28:**

Devine discusses the system of claim 18, further comprising:

means for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

**As per claim 29:**

Devine teaches a system for placing a process executed in a node in a security context, comprising:

a server; and **(col.8, line 25)**

a sending node comprising:

a transmission module that transmit a request to the server to verify a username and a node identification **(col.12, lines 36-37)**, and receives security context information from the server in response to the request, wherein the security context information comprises a virtual address for the sender node; **(col.23, lines 26-28 and col.27, lines 47-60)**

**[The message includes the user identifier (username) and the virtual address. In addition, the session information, proxy specific data, the target proxy identifier (col.13, lines 48-67), and the socket type and port number of which identifies the node (col.26, lines 24-29). It is obvious that a secure session comprises the message which would include a node identification and an address in order to identify and determine the proper system that it is communicating to, else the session would be not be considered secure (col.11, lines 41-43).]**

memory containing a process and an associated process table; and **(col.13, lines 60-67)**

an appending module that appends the received security context information and the node identification for the process in the process table. **(col.13, line 43 thru col.14, line 17)**

**As per claim 30:**

Devine discloses the system of claim 29, wherein the transmission module further receives a key that corresponds to the node identification from the server. **(col.8, lines 52-55)**

**As per claim 31:**

The system of claim 30, further comprising:

an encryption module that encrypts a packet transmitted by the process using the key; **(col.9, lines 6-13)**

an encapsulating module that encapsulates the encrypted packet with a header that comprises the node identification. **(col.13, lines 31-67)**

**As per claim 32:**

The system of claim 29, further comprising:

a gateway that provides communication between the process and a second process executing in the node, and **(col.22, lines 21-22)**

wherein the transmission module further sends a second request to the server to verify a username and node identification **(col.10, lines 39-44)**, and receives additional security context information from the server **(col.23, lines 61-63)**, wherein the additional security context information comprises a second virtual address for the node; **(col.24, lines 60-64)**

appending the security context information for the second process in a process table that is associated with the second process. **(col.13, line 43 thru col.14, line 17)**

**As per claim 33:**

Devine teaches a system for providing secure communications between a first process, comprising:

means for obtaining a node identification and a virtual address; **(col.9, lines 2-10 and col.23, lines 61-64)**

**[The message includes the user identifier (username) and the virtual address. In addition, the session information, proxy specific data, the target proxy identifier (col.13, lines 48-67), and the socket type and port number of which identifies the node (col.26, lines 24-29). It is obvious that a secure session comprises the message which would include a node identification and an address in order to identify and determine the proper system that it is communicating to, else the session would be not be considered secure (col.11, lines 41-43).]**

means for including the node identification and the virtual address in a field corresponding to the first process in a process table; **(col.14, lines 7-11 and col.23, lines 61-63)**

means for transmitting a datagram that contains the node identification and the virtual address from the first process to a socket; and **(col.24, lines 60-64)**

means for receiving the datagram at the second process that contains the node identification and a second virtual address. **(col.14, lines 7-11 and col.23, lines 61-64)**

**As per claim 34:**

Devine discloses the system of claim 33, wherein means for obtaining a node identification and a virtual address further comprises:

means for modifying a socket structure in the socket so that the socket structure accepts the node identification and the virtual address; and

**(col.13, lines 31-67)**

means for modifying a process table so that the table comprises a node identification field and a virtual address field. **(col.23, lines 26-31 and col.26, lines 24-31)**

memory containing a process and an associated process table; and

**(col.13, lines 60-67)**

an appending module that appends the received security context information and the node identification for the process in the process table.

**(col.13, line 43 thru col.14, line 17)**

**As per claim 35:**

Devine discloses a computer readable medium for controlling a data processing system to perform a method for providing communication access between a first process and a second process, comprising:

an appending module for appending security context information for the first process in a process table; **(col.9, lines 60-63 and col.13, lines 60-67)**

an opening module for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

a transmitting module for transmitting a packet from the first process to the second process through the open socket, the packet comprising the security context information for the first process in the process table;

**(col.14, lines 6-11)**

determining if the first and second process belong to a channel; and

**(col.9, lines 1-420, lines 53-63)**

accepting the transmitted packet when the first and second process belong to the channel. **(col.22, lines 53-67 and col.23, lines 7-16)**

**[Devine discloses once the client session is determined to be secure and the message with valid security information, the user is entitled to communicate with the desired connection. It is obvious the session is mapped to the targeted destination for Devine discloses that the validation is performed to make sure that the user is entitled to communicate with the desire service (col.9, lines 1-21). Further, since the request is mapped to the associated session, it is obvious that the session refers to a target system, which is the associated to a channel, destination/target address, and socket that belongs to the associated target system. Plus, Devine discloses a key is necessary to validate the**

**first and second process, which the key identifies and validates the particular process that obviously allows communication to the associated system. Thus, it would have been obvious to determine if the process belongs to a channel and accepting the transmitted packet that belong to the channel is establishing that the session is secure by having the proper key that identifies the associated session.]**

**As per claim 36:**

The computer readable medium of claim 35, further comprising a modifying module for modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

**As per claim 37:**

The computer readable medium for claim 35, further comprising:

a received module for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

a verifying module for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

a permitting module for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

**As per claim 39:**

The computer readable medium of claim 38, wherein the determining module comprises:

a comparing module that compares the security context information in the received packet and security context information in another process table. **(col.27, line 43 thru col.28, line 5)**

**As per claim 40:**

The computer readable medium of claim 39, wherein the process table and the another process table are located on a single node. **(col.9, lines 60-66)**

**As per claim 41:**

The computer readable medium of claim 37, wherein the verifying module comprises:

a determining module for determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

a permitting module for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

**As per claim 42:**

The computer readable medium of claim 41, wherein the determining module comprises a initiating module that initiates a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

**As per claim 43:**

The computer readable medium of claim 41, wherein the permitting module comprises:

a decrypting module for decrypting the packet on a node; and **(col.12, lines 34--37)**.

an authenticating module for authenticating a sender associated with the first process on the node. **(col.8, lines 27-28)**

**As per claim 44:**

The computer readable medium of claim 35, wherein the appending module comprises:

an obtaining module for obtaining the security context information from a third process, the security context comprising a virtual address and a node identification; and

**(col.9, lines 2-10 and col.23, lines 61-64)**

a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

**As per claim 45:**

The computer readable medium of claim 35, further comprising:

a modifying module for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

***Response to Amendment***

After reviewing Applicant's arguments and Applicant indicating that the Examiner equates a "channel" to "client session", the Examiner maintains the rejection with the teachings of Devine, et al.

Devine teaches establishing a secure messaging session (process) with one of the servers via an Internet secure communications path established with a secure sockets SSL version of HTTPS by decrypting the message with the session key, verifying the user session, and after establishing the request is of a valid user maps the request to it associated session (col.8, lines 22-32). Devine's invention reciprocates the successful authentication process with allowing a connection to the targeted destination (col.9, lines 1-21). The session is mapped to the associated channel, destination/target address, and socket that belongs to the associated target system (col.11, lines 41-43). Hence, Devine discloses the process of determining if the first and second process belong to a channel by determining if it is a secure client session which involves the client requesting and validating the request (as discussed above) which in essence secures the message session which then maps to the connection that the session belongs to (col.13, lines 60-64). The client session is not a channel, but when Devine discloses the term "session", it merely involves the appropriate server or system, its address (col.22, lines 25-30 and 53-66), its communications link or channel, and its socket (col.26, lines 15-35).

Plus, a key is necessary to validate the first and second process, which the key identifies and validates the particular process that obviously allows communication to the associated system. Thus, the session that has been validated with the proper key determines if the process belongs to a channel.

In addition of validating the session, the message includes the user identifier (username) and session information, proxy specific data (which is the socket, port number) that identifies the node, and the target proxy identifier and the virtual address (col.23, lines 25-28). It is obvious that a secure session comprises the message include a node identification and an address in order to identify and determine the proper system that it is communicating to, else the session would be not be considered secure.

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax

phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*****TC 2100 will be moved to Carlyle in October 2004. At this time, any inquiry or communications should be directed to the examiner, LEYNNA HA, whose new telephone number is (571) 272-3851 and the new telephone number for TC 2100 receptionist is 571-272-2100.**

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100